

# Fr. Heil VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

Absender: INTERNATIONALE RECHERCHENBEHÖRDE

An:

CT IPS AM Mch P

PCT

siehe Formular PCT/ISA/220

MAY 12 2005

IP

time limit

27. 09. 05

SCHRIFTLICHER BESCHIED DER  
INTERNATIONALEN

RECHERCHENBEHÖRDE

(Regel 43bis.1 PCT)

Absendedatum

(Tag/Monat/Jahr) siehe Formular PCT/ISA/210 (Blatt 2)

Aktenzeichen des Anmelders oder Anwalts

siehe Formular PCT/ISA/220

8003P/1803600

**WEITERES VORGEHEN**

siehe Punkt 2 unten

Internationales Aktenzeichen

PCT/EP2004/052885

Internationales Anmeldedatum (Tag/Monat/Jahr)

09.11.2004

Prioritätsdatum (Tag/Monat/Jahr)

27.11.2003

Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK

H04M1/253, H04L9/08, H04L9/00, H04M7/00, H04K1/00

Anmelder

SIEMENS AKTIENGESELLSCHAFT

1. Dieser Bescheid enthält Angaben zu folgenden Punkten:

- ☒ Feld Nr. I Grundlage des Bescheids
- ☐ Feld Nr. II Priorität
- ☐ Feld Nr. III Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit
- ☐ Feld Nr. IV Mangelnde Einheitlichkeit der Erfindung
- ☒ Feld Nr. V Begründete Feststellung nach Regel 43bis.1(a)(i) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung
- ☐ Feld Nr. VI Bestimmte angeführte Unterlagen
- ☐ Feld Nr. VII Bestimmte Mängel der internationalen Anmeldung
- ☐ Feld Nr. VIII Bestimmte Bemerkungen zur internationalen Anmeldung

2. **WEITERES VORGEHEN**

Wird ein Antrag auf internationale vorläufige Prüfung gestellt, so gilt dieser Bescheid als schriftlicher Bescheid der mit der internationalen vorläufigen Prüfung beauftragten Behörde ("IPEA"); dies trifft nicht zu, wenn der Anmelder eine andere Behörde als diese als IPEA wählt und die gewählte IPEA dem Internationale Büro nach Regel 66.1bis b) mitgeteilt hat, daß schriftliche Bescheide dieser Internationalen Recherchenbehörde nicht anerkannt werden.

Wenn dieser Bescheid wie oben vorgesehen als schriftlicher Bescheid der IPEA gilt, so wird der Anmelder aufgefordert, bei der IPEA vor Ablauf von 3 Monaten ab dem Tag, an dem das Formblatt PCT/ISA/220 abgesandt wurde oder vor Ablauf von 22 Monaten ab dem Prioritätsdatum, je nachdem, welche Frist später abläuft, eine schriftliche Stellungnahme und, wo dies angebracht ist, Änderungen einzureichen.

Weitere Optionen siehe Formblatt PCT/ISA/220.

3. Nähere Einzelheiten siehe die Anmerkungen zu Formblatt PCT/ISA/220.

Name und Postanschrift der mit der internationalen  
Recherchenbehörde



Europäisches Patentamt - Gitschiner Str. 103  
D-10958 Berlin  
Tel. +49 30 25901 - 0  
Fax: +49 30 25901 - 840

Bevollmächtigter Bediensteter

Carnerero Álvaro, F

Tel. +49 30 25901-469



**SCHRIFTLICHER BESCHEID DER  
INTERNATIONALEN RECHERCHEBEHÖRDE**Internationales Aktenzeichen  
PCT/EP2004/052885

1AP20 Rec'd PCT/PTO 30 MAY 2006

**Feld Nr. I Grundlage des Bescheids**

1. Hinsichtlich der **Sprache** ist der Bescheid auf der Grundlage der internationalen Anmeldung in der Sprache erstellt worden, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.
  - ☐ Der Bescheid ist auf der Grundlage einer Übersetzung aus der Originalsprache in die folgende Sprache erstellt worden, bei der es sich um die Sprache der Übersetzung handelt, die für die Zwecke der internationalen Recherche eingereicht worden ist (gemäß Regeln 12.3 und 23.1 b)).
2. Hinsichtlich der **Nucleotid- und/oder Aminosäuresequenz**, die in der internationalen Anmeldung offenbart wurde und für die beanspruchte Erfindung erforderlich ist, ist der Bescheid auf folgender Grundlage erstellt worden:
  - a. Art des Materials
    - ☐ Sequenzprotokoll
    - ☐ Tabelle(n) zum Sequenzprotokoll
  - b. Form des Materials
    - ☐ in schriftlicher Form
    - ☐ in computerlesbarer Form
  - c. Zeitpunkt der Einreichung
    - ☐ in der eingereichten internationalen Anmeldung enthalten
    - ☐ zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht
    - ☐ bei der Behörde nachträglich für die Zwecke der Recherche eingereicht
3. ☐ Wurden mehr als eine Version oder Kopie eines Sequenzprotokolls und/oder einer dazugehörigen Tabelle eingereicht, so sind zusätzlich die erforderlichen Erklärungen, daß die Information in den nachgereichten oder zusätzlichen Kopien mit der Information in der Anmeldung in der eingereichten Fassung übereinstimmt bzw. nicht über sie hinausgeht, vorgelegt worden.
4. Zusätzliche Bemerkungen:

---

**Feld Nr. V Begründete Feststellung nach Regel 43*bis*.1(a)(i) hinsichtlich der Neuheit, der  
erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur  
Stützung dieser Feststellung**

---

**1. Feststellung**

Neuheit	Ja: Ansprüche 1-10 Nein: Ansprüche
Erfinderische Tätigkeit	Ja: Ansprüche Nein: Ansprüche 1-10
Gewerbliche Anwendbarkeit	Ja: Ansprüche: 1-10 Nein: Ansprüche:

**2. Unterlagen und Erklärungen:**

**siehe Beiblatt**

1. In diesem Prüfungsbericht werden folgende, im Internationalen Recherchenbericht zitierte Dokumente (D) genannt:

- D1: US-B1-6 356 638 (HARDY DOUGLAS ALLAN ET AL) 12. März 2002 (2002-03-12)**  
**D2: SCHNEIER B: "APPLIED CRYPTOGRAPHY, PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C" JOHN WILEY & SONS, 1996, XP002322926 NEW YORK, US ISBN: 0-471-11709-9**  
**D3: LU W P ET AL: "SECURE COMMUNICATION IN INTERNET ENVIRONMENTS: A HIERARCHICAL KEY MANAGEMENT SCHEME FOR END-TO-END ENCRYPTION" IEEE TRANSACTIONS ON COMMUNICATIONS, IEEE INC. NEW YORK, US, Bd. 37, Nr. 10, 1. Oktober 1989 (1989-10-01), Seiten 1014-1023, XP000070200 ISSN: 0090-6778**  
**D4: US-B1-6 584 562 (FIORI COSTANTINO) 24. Juni 2003 (2003-06-24)**  
**D5: TANENBAUM A S: "COMPUTER NETWORKS, PASSAGE" COMPUTER NETWORKS, LONDON : PRENTICE-HALL INTERNATIONAL, GB, 1996, XP002322927 ISBN: 0-13-394248-1**  
**D6: US-A-5 778 071 (CAPUTO ET AL) 7. Juli 1998 (1998-07-07)**

2. Die vorliegende Anmeldung erfüllt nicht die Erfordernisse des Artikels 33 PCT, weil der Gegenstand der Ansprüche nicht auf einer erfinderischen Tätigkeit im Sinne von Artikel 33(3) PCT beruht.

- 2.1 Das Dokument D1 offenbart ein System zum Verschlüsseln von Telefongesprächen zwischen einem oder mehreren Endgeräten in einem paketorientierten Datennetz und einem oder mehreren Endgeräten in einem analogen Telefonfestnetz, wobei das paketorientierte Netz und das Telefonnetz über einen Zugangsrechner miteinander verbunden sind, und wobei die Verschlüsselung und der ihr vorausgehende Schlüsselaustausch gemäss dem Ende-zu-Ende-Prinzip durchgeführt werden.

(Das Dokument D1 erwähnt auch die Tatsache, dass alle Endgeräte über das notwendige Verschlüsselungshardware verfügen müssen. Siehe z.B. Spalte 2, Zeilen 50-63. Dies beinhaltet die Möglichkeit der "Zwischenschaltung" eines eigens vorgesehenen Sicherheitsmoduls. Im Zweifelsfall, siehe das Dokument D6,

Zusammenfassung und Abbildung 3).

Was von D1 nicht explizit offenbart wird ist die Verwendung während der obigen Ende-zu-Ende-Sitzung der im paketorientierten Netz üblichen Algorithmen und Protokolle zum verschlüsselten Datentransport und zum Schlüsselaustausch.

- 2.2 Das Dokument D2 ist einem wohlbekannten Nachschlagewerk entnommen, dessen Inhalt vom Fachmann ohne erfinderisches Zutun herangezogen werden kann (vgl. die PCT Richtlinien, PCT/GL/ISPE 13.13). Es beschreibt das Prinzip der Ende-zu-Ende-Verschlüsselung zwischen Telekommunikationsendgeräten (Seiten 216-220). Dabei erwähnt es (Seite 219) die erforderliche Verwendung desselben Verschlüsselungsalgorithmus in beiden Endgeräten, sowie die Notwendigkeit der Aushandlung eines gemeinsamen kryptografischen Schlüssels zwischen den Endgeräten anhand eines von ihnen unterstützten Schlüsselaustauschprotokolls.

Es wäre daher für den Fachmann nahe liegend, zur Gewährleistung der Kompatibilität alle potentiell an den besagten gesicherten Ende-zu-Ende-Sitzungen beteiligten Endgeräte mit Hardware (bzw. Software) auszustatten, das die zu transportierenden Daten gemäss den im paketorientierten Datennetz üblichen Algorithmen und Protokollen verarbeiten kann.

Daraus folgt, dass dem Gegenstand des unabhängigen Anspruchs keine erfinderische Tätigkeit zugrunde liegt (Artikel 33(3) PCT).

- 2.3 Die Kompatibilitätsprobleme die der Aufbau von sicheren Ende-zu-Ende-Verbindungen darstellt sind dem Fachmann nicht nur aus D2 bekannt. Siehe z.B. D3, Seiten 1014 und 1015 oder D4, Spalte 1, Zeile 59 bis Spalte 2, Zeile 13. Der Inhalt von diesen Dokumenten eignet sich ebenfalls zur Formulierung ähnlicher Einwände hinsichtlich der Erfordernisse von Artikel 33(3) PCT.
- 2.4 Es gilt zudem zu beachten, dass die folgenden in den abhängigen Ansprüchen enthaltenen Merkmale dem Fachmann bekannt sind:

-Das Führen von Telefongesprächen zwischen Endgeräten in einem IP-Datennetz

und Endgeräten in einem Telefonnetz (TDM);

-Die Übertragung von Daten über ISDN-Telefonnetze. Siehe D5, Seiten 139-144 (es handelt sich dabei ebenfalls um ein bekanntes Nachschlagewerk);

-Der Aufbau von Modemverbindungen (über die eine PPP-Verbindung läuft) um IP-Datenpakete zu transportieren (D5, Seiten 229-232).